DETAILED ACTION

1. This is in response to the amendment filed on 14 August 2007.

2. Claims 26, 31-34, 40-42 and 44-49 are pending in the application.

3. Claims 26, 31-34, 40-42 and 44-49 have been allowed.

4. Claims 1-25, 27-30, 35-39, 43 and 50-63 have been cancelled.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Andrew J. Curtin on 23 October 2007.

The application has been amended as follows:

Claim 26 (Amended) A method of providing security in a network having a network interface device that makes a network connection without a firewall capability in said network interface device that is required by the network for data transfer between the network and a host device using the network interface device, said method comprising:

a) allowing, by said network, a connection to said network to be established when the host device uses said network interface device without the required firewall capability only if a firewall device comprising a hardware implemented firewall is coupled to said host device and a configuration integrity check of a software component on said host device passes;

b) receiving data from said network over said connection establish via said network interface device;

c) processing said data with said hardware implemented firewall; and

d) transferring said processed data to said host device;

wherein, performing said configuration integrity check by performing a hash on said software component to produce a hash value and comparing said hash value with a stored hash value,

wherein, said stored hash value resides on said firewall device.

Claim 27 (Cancelled)

Claim 28 (Cancelled)

Response to Amendment

6. The examiner approves of the amendment made to claims 26 and 40. The applicant has amended the preamble of claims 26 and 40 to recite "in said network interface device" instead of "in said communication interface device". This amendment overcomes the rejection under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The examiner withdraws the rejection under lack of antecedent basis. The applicant's amendment has clarified the limitation "allowing a connection to said network to be established when said host device uses said network interface device without the required firewall capability only if a firewall device comprising a hardware implemented firewall is coupled to said host device". The claim has been amended so that the network allows the connection. The applicant has removed the

limitation "performing a configuration integrity check of a software component on a host device, wherein said configuration integrity check is performed before said network connection is allowed, wherein said connection is allowed only if said configuration integrity check passes". This amendment resolves the issue of why an integrity check for a network connection would take place after a connection has been allowed to the network.

Allowable Subject Matter

7. Claims 26, 31-34, 40-42 and 44-49 are allowed.

The following is an examiner's statement of reasons for allowance:

The current application is directed towards a system for providing security in a computing network. The system has a server for distributing policies to be implemented by firewall devices in the network. The firewall devices provide hardware implemented firewalls to communication devices making network connections. The system has logic to allow a connection to be made to the network via a communication device at a node provided the firewall device is at that node. Therefore, the firewall device must be in the system for a connection to be established via the communication device. Additionally, the system is configured to cause data transferred by the communication device to be processed by the firewall.

Independent claims 26 and 40 are directed towards a method of providing security in a network having a network interface device that makes a network connection without a firewall capability in the network interface device that is required by the network for data transfer between the network and a host device using the network interface device.

The closest prior art to the current application was Spain et al U.S. Patent No. 7,058,811 B2 (hereafter Spain). Spain is directed towards a hardware authenticity verification system includes a hardware element having a hardware address. A digital signature generator is included to create a digital signature of the hardware address of the hardware element. A memory element stores the digital signature of the hardware element. A software program is included to compare the digital signature of the hardware element to a known value. If the digital signature of the hardware element matches the known value, the user may be granted read and write access to all memory locations within the memory element, including a location in which the hardware address is stored. On the other hand, if the hardware address of the hardware element does not match the known value, the hardware element will not properly function, because the manufacturer's software program is configured to not load on the hardware element if the hardware address of the hardware element does not match the known value.

However, Spain differs from the current application. Spain does not disclose, teach or fairly suggest allowing, by a network, a connection to the network to be established when the host device uses a network interface device without the required firewall capability only if a firewall device comprising a hardware implemented firewall is coupled to the host device and a configuration integrity check of a software component on the host device passes. Spain does not disclose, teach or fairly suggest that performing a hash on the software component to produce a hash value and comparing the hash value with a stored hash value perform the integrity check. Spain does not disclose, teach or fairly suggest that the stored hash value resides on the firewall device.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431

William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431

/